2024 1st International Conference on Emerging Technologies for Dependable Internet of Things (ICETI) | 979-8-3315-3355-7/24/$31.00 ©2024 IEEE | DOI: 10.1109/ICETI63946.2024.10777136

Challenges and Opportunities in Healthcare and Industrial IoT: A Comparative Analysis

Zaid Berjis
Electrical and Computer Engineering Department
College of Engineering
University of Duhok
Duhok, Iraq
zaid.berjis@uod.ac

Siddeeq Y. Ameen
Energy Engineering Department
College of Technical Engineering, Duhok Polytechnic University, Duhok, Iraq
Siddeeq.ameen@dpu.edu.krd

Mohammed H. Al-Jammas
Computer and Information Engineering Department
College of Electronics, Ninevah University,Mosul, Iraq
mohammed.aljammas@uonineveh.edu.iq

Abstract— The Internet of Things (IoT) has changed many industries by enabling smart devices to transmit data, operate autonomously, and interact in real-time. Among its most prominent applications are in healthcare and industrial sectors, where IoT is classified into two classes: massive Machine-Type Communication (mMTC) and Ultra-Reliable Low Latency Communication (URLLC). While mMTC devices prioritize low energy consumption and can handle large-scale deployments with minimal data rates, URLLC devices are focused on mission-critical applications requiring ultra-low latency and high reliability. This paper examines the challenges and opportunities of IoT implementation in healthcare and industrial sectors, focusing on interoperability, data security, and scalability issues. The objective is to provide actionable solutions for the effective integration of IoT technologies. The investigation shows that in healthcare, mMTC is utilized for non-critical monitoring, while URLLC supports critical tasks like remote surgery. In industrial settings, mMTC improves processes like supply chain management, while URLLC enables automation and real-time control of machinery. Despite these opportunities, challenges such as data privacy, security, interoperability, and reliability remain. Addressing these issues is crucial for unlocking the full potential of IoT in healthcare and industrial sectors.

Keywords— IoT, healthcare, industrial IoT, mMTC, URLLC, real-time processing, automation, low latency, reliability.

I. INTRODUCTION

The Internet of Things (IoT) refers to the collection of devices that are connected to the network or interconnected to each other or both communicating to the network and to each other. They can transmit and receive data, besides being able to act without a human interaction [1]. These devices are enabled by attaching sensors to them and software capabilities and wireless communication to allow them to run autonomously, and making those devices able to have real-time interaction with the environment they are set in, so they add to their value by controlling and automating tasks [2]. As predicted by [3], the number of IoT devices is projected to reach 75 billion by 2025, indicating a massive shift towards connected ecosystems. IoT devices are imbued with wireless connectivity, which is both a pro and a con. On one hand, wireless communication capability enhances flexibility. The flexibility refers to the adaptability of IoT devices to various environments, and use cases allowing IoT devices to work in multiple settings. On the other hand, wireless communication comes with a list of challenges that could impact the dependability, where dependability refers to the ability of IoT devices to perform reliably, consistently and securely over time. It encompasses key attributes of trustworthiness of such devices, including, latency issues, security, and also energy consumption concerns that need to be addressed especially in places that are classified as critical e.g. in healthcare and industrial applications [4].

IoT devices can be broadly put into two main categories: massive Machine-Type Communication (mMTC) or massive IoT, and Ultra-Reliable Low Latency Communication (URLLC) or critical IoT [5]. mMTC devices are characterized by having low data rate, infrequent data generation, low power consumption, making them ideal for simple sensors monitoring the environment [6]. On the contrary, URLLC devices require high reliability. The reliability can be defined as the likelihood that IoT devices will perform their intended functions without failure under specified conditions for a given period. This is crucial in applications like healthcare monitoring or industrial automation, where device failure could have serious consequences. The low latency is very important since IoT role is to operate for mission-critical applications like industrial automation, smart cities, and healthcare, where data must be processed in real-time [7].

This paper aims to lay out the challenges and opportunities related to the healthcare and industrial sectors' use of IoT devices. It discusses how mMTC and URLLC IoT applications are implemented in those sectors, the main challenges they encounter and how to alleviate or solve these challenges.

II. CLASSIFICATION OF IOT DEVICES

IoT devices are mainly divided into two group types, each has its own characteristics and use cases.

A. Massive Machine-Type Communication (mMTC)

It refers to a large number of connected devices, usually in millions, but they generate a small amount of data. They can be used in applications where real-time data processing is not required, like in a temperature sensor, smart meter, and other

979-8-3315-3355-7/24/$31.00 ©2024 IEEE

environmental monitors. Fig.1 shows a typical mMTC communication architecture [8].

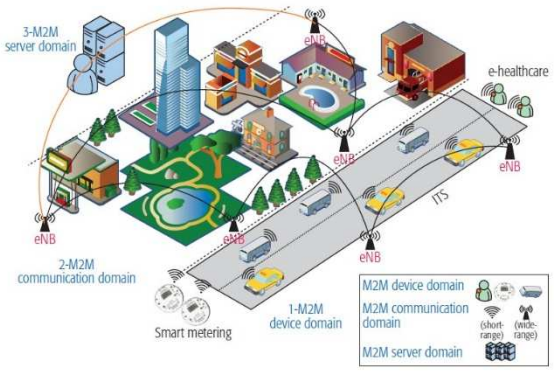

Fig. 1: mMTC Communication Architecture

mMTC devices are typically used in remote areas or inaccessible locations for long periods of time with the need for maintenance, so being energy-efficient is of crucial importance. Equation 1 shows the total energy usage of a device based on its mode of operation (transmission, reception, idle, and sleep) [9].

$$E_{total} = P_{tx}T_{tx} + P_{rx}T_{rx} + P_{idle}T_{idle} + P_{sleep}T_{sleep} \quad (1)$$

where P_{tx} is power of transmission mode, T_{tx} is the time duration of transmission mode, P_{rx} is the power of reception mode, T_{rx} is the time duration of reception mode, and so on for idle and sleep modes.

In the healthcare sector, wearable fitness trackers, and remote health monitoring devices are typical mMTC applications. These devices generate data that do not need real-time action rather those data are useful for long-term analysis and monitoring. Table I gives a summary of some of these devices and their power consumption, coverage area, and expected operational lifetimes [10].

TABLE I: SUMMARY OF SOME DEVICES PARAMETERS

Device Type	Power Consumption	Coverage Area	Lifetime (years)
Smart Meter	Low	Wide	10-15
Environmental Monitor	Very Low	Rural/Urban	10-20
Wearable Health Tracker	Low	Short-Range	5-10
Remote Sensor (Agriculture)	Very Low	Wide (Rural)	5-15

The maximum number of devices that an mMTC network can support is estimated using the following network capacity equation:

$$N = \frac{B \times \eta}{Data\ Rate\ per\ device} \quad (2)$$

where;

B is the available bandwidth

η is the spectral efficiency

Finally, Table II compares between different mMTC protocols of communication, such as NB-IoT, LoRaWAN, LTE-M, and Sigfox, focusing on frequency band, data rate, energy consumption, and coverage area [11].

TABLE II: MMTC PROTOCOLS OF COMMUNICATION

Parameter	NB-IoT	LoRaWAN	LTE-M	Sigfox
Frequency Band	Licensed	Unlicensed	Licensed	Unlicensed
Data Rate	Low	Low	Moderate	Low
Latency	High	High	Moderate	High
Energy Consumption	Very Low	Very Low	Low	Very Low
Deployment Range	Large	Large	Medium	Large
Typical Application	Smart Meter	Environment	Healthcare	Tracking

B. *Ultra-Reliable Low Latency Communications (URLLC) or Critical IoT*

The main reason for the development of URLLC is to be used for mission-critical applications where high reliability and low latency are top priority. Real-time data processing of a huge amount of data is those systems' central role. Fig. 2 shows an overview of URLLC [12].

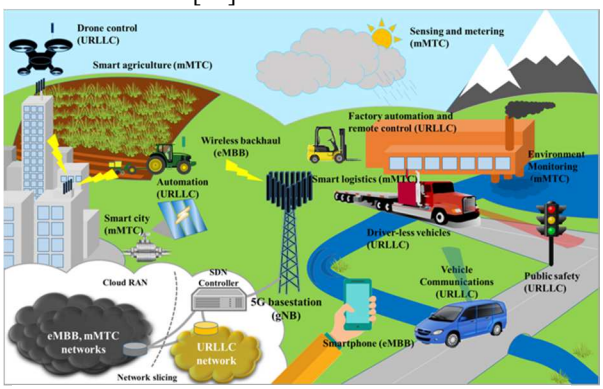

Fig. 2: An Overview of URLLC

Latency-reliability tradeoff graph shown in Fig.3 is the best description of the stringent requirements of URLLC.

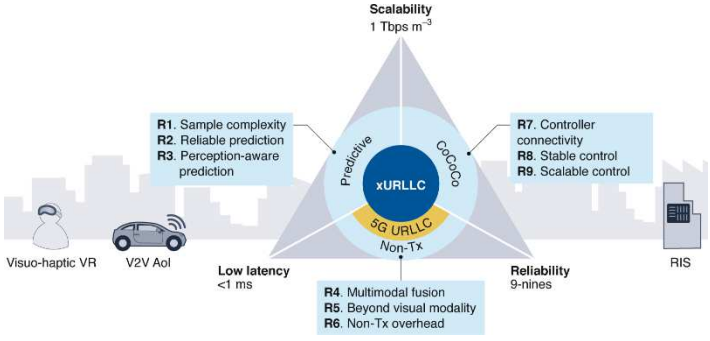

Fig. 3: Latency – Reliability Tradeoff

To calculate the end-to-end latency of a URLLC equation 3 can be used:

$$Latency_{total} = \frac{L}{R} + \frac{Processing\ Time}{n} + Propagation\ Delay \quad (3)$$

where:

L is the length of the message.

R is the transmission rate.

n is the number of processing nodes.

Processing Time refers to the computational delay at each node.

Some use cases of various URLLC are summarized in Table III, showing applications as autonomous vehicles and industrial robots need latency equal or lower than 1ms with five-9 reliability [13]. One of the major roles URLLC is in the healthcare sector specifically in telemedicine. For example, remote surgery and real-time patient monitoring. These systems depend mainly on extreme low-latency communication to secure an interrupted operation.

TABLE III: URLLC USE CASES

Application	Latency required (ms)	Reliability %	Data Rate (Mbps)
Autonomous Vehicle	<1	99.999	High
Industrial Robots	1-10	99.999	Moderate
Remote Surgery	<1	99.999	High
Real-Time Patient Monitoring	<10	99.99	Moderate

In industrial IoTs, applications of URLLC include automated machinery and robotics where even a little delay can have a bad consequence and fatal accident. The probability of error of a URLLC system can be found by using [14]:

$$P_{error} = \frac{1}{T_{packet} \times R_{retransmission}} \quad (4)$$

where:

T_{packet} is the packet transmission time.

$R_{retransmission}$ is the retransmission rate.

Equation 4 shows the need to minimize both transmission time and the need for retransmission in applications of critical IoT. To highlight the superiority of URLLC through parameters like latency, reliability, and data rate compared to other communication technologies like Wi-Fi 6 and Ethernet, Table IV is constructed [15].

TABLE IV: COMMUNICATION TECHNOLOGIES COMPARISON

Feature	5G URLLC	Wi-Fi 6	Ethernet
Latency	1 ms	10 ms	1-10 ms
Data Rate	High	Moderate	High
Reliability	99.999%	99.9%	99.99%
Typical Application	Critical IoT	IoT,Home	Industrial

III. IOT APPLICATIONS IN HEALTHCARE

IoT has transformed healthcare by enabling medical personnel to monitor patients continuously, remotely make diagnostics, and prepare customized treatment plans. The ecosystem created by IoT is exceptional where patient data can be collected in real-time, analyzed, and better decision are made for the benefit of patient [16].

A. mMTC Applications in Healthcare

In healthcare, devices such as wearable fitness tracker, remote patient monitoring, and noncritical health sensors are all applications of mMTC IoT [17]. The data collected by these devices are not of large amounts, such as heart rate, temperature, timings of sleep, these data are sent to the healthcare provider to analyze them and make informed decision about the patient's health [17].

The main challenges for mMTC healthcare devices

- Data Privacy: considering the amount of sensitive data that can be collected from a population of patients, data privacy is crucial [18].
- Battery Life: for many of those devices frequent charging could be cumbersome, so long battery life is critical [19].
- Interoperability: IoT devices' heterogeneity and different manufacturing sources make it difficult to integrate all devices in one ecosystem [20].

B. URLLC Applications in Healthcare

URLLC is used in healthcare applications were real-time data processing is required. Remote surgery, telemedicine, intensive care unit patient monitoring, are few examples of such devices that use URLLC [21].

The main challenges of URLLC healthcare devices are

- Reliability: minimizing downtime and transmission delays is essential [21].
- Latency: Remote surgery could endure severe consequences if latency exceeds a fraction of a second [22].
- Security: cyberattacks on such IoT devices are disruptive and could lead to a drastic negative impact [23].

IV. IOT APPLICATIONS IN INDUSTRY

IoT in industry is called Industrial IoT (IIoT), focuses on enhancing productivity, reducing downtime, and optimize their processes. It connects machines, sensors, and control systems. The methods involve automation, real-time monitoring, and predictive maintenance [24].

A. mMTC Applications in Industrial IoT

IoT sensors can track the movement of goods through supply chain reducing delays and ensuring timely delivery. Industrial IoT can for example monitor the temperature and humidity in a warehouse.

The main challenges of mMTC in Industrial IoT are;

- Scalability: millions of devices enter the market each year make managing them a challenge [25].

- Power Efficiency: the places that these devices are deployed usually are in remote areas and hazardous environment [26].
- Data Overload: efficient data management schemes must be chosen to avoid data overload since data are coming from millions of devices [27].

B. URLLC in Industrial IoT

URLLC play a crucial role in real-time control of large factories and automation in industrial settings. Some examples are autonomous robots, real-time quality control system, and automated manufacturing processes. To ensure the safety and efficiency of those devices' high reliability and low latency communication is essential [26].

The main challenges of URLLC in Industrial IoT are;

- Reliability: any downtime in IIoT can be very costly [26].
- Latency: robotic arms in factories require real-time response and feedback to operate flawlessly [24].
- Cybersecurity: to protect critical infrastructure a robust measures are required to prevent cyberattacks [23].

C. Case Studies

- Case Study 1: The city of Barcelona's smart city initiative, where IoT has been deployed in areas like waste management and transportation, has resulted in significant cost savings. However, it faced initial resistance due to privacy concerns and required robust public communication strategies [29].
- Case Study 2: General Electric's (GE) use of IoT in its "Digital Twin" technology for predictive maintenance in the aviation industry has reduced downtime but encountered challenges in real-time data processing, later resolved by edge computing [30].

D. Other Challenges

Here we present few challenges that rise because of geographic location.

- Developing Countries: In regions with less reliable connectivity, IoT deployment is hindered by poor internet infrastructure and high costs, limiting its adoption in areas like agriculture or smart cities.
- Geographic-Specific Security Challenges: In areas with high levels of cybercrime, like certain parts of North America and Europe [28], IoT systems are at higher risk of cyber-attacks. This necessitates more robust security measures tailored to the local risk environment.

Specific Applications: here we present challenges due to the specific applications they serve

- Smart Cities: Urban IoT applications must deal with different regulations and privacy standards in different jurisdictions. For example, privacy regulations in Europe (GDPR) might impose more stringent requirements on IoT data collection than in other parts of the world.
- Manufacturing: In highly automated manufacturing plants, the need for real-time, low-latency IoT systems may be more pronounced than in other industries, requiring cutting-edge solutions like 5G and edge computing.

V. Analysis of Challenges and Opportunities

A. Challenges in IoT healthcare and IIoT

TABLE V: DIRECT COMPARISON BETWEEN THE CHALLENGES OF IOT DEVICES IN HEALTHCARE AND INDUSTRY

Challenges	IoT in Healthcare	IoT in Industrial Settings
Data Privacy	Sensitive patient data collection and storage pose risks to privacy [18].	Industrial data (e.g., supply chains) may be compromised by cyber-attacks [23].
Battery Life	Wearable devices need long battery life for continuous monitoring [19].	Devices in remote or hazardous locations require high energy efficiency [26].
Interoperability	Devices from different manufacturers struggle to integrate into one system [20].	Different systems in large factories may not communicate seamlessly [20].
Reliability	High reliability is crucial, especially for applications like remote surgery [21].	Downtime can be costly in factory automation, requiring ultra-high reliability [26].
Latency	Remote surgery and telemedicine need extremely low-latency communication [22].	Robotic arms and real-time control systems require low latency [24].
Security	Cyber-attacks on healthcare IoT can cause severe consequences [23].	Critical infrastructure is vulnerable to cyber-attacks and needs robust protection [23].
Scalability	As the number of devices grows, managing large-scale healthcare IoT is challenging.	Managing millions of industrial IoT devices, especially in supply chains, is difficult [25].
Power Efficiency	Medical devices must be energy-efficient to operate in remote or continuous settings.	Power-efficient IoT devices are critical in remote or hazardous environments [26].
Data Overload	Healthcare IoT generates vast amounts of data that need effective management [27].	Industrial IoT must manage large volumes of data coming from millions of devices [27].
Geographic Challenges	IoT adoption in developing countries faces poor infrastructure and high costs [28].	Industrial IoT deployment may face connectivity issues in remote locations.

B. Challenges Solutions

Here are a few steps to tackle the challenges mentioned above:

1) Security Challenges:

- Encryption: Use lightweight options like ECC or post-quantum cryptography.
- Zero-Trust Architecture: assuming that all devices and users are potential threats

- Blockchain: Using blockchain's decentralized ledger, IoT devices can verify and authenticate data transactions without relying on a central authority, minimizing the risk of tampering.
- Intrusion Detection Systems (IDS): Implementing AI-driven IDS that can monitor IoT networks for suspicious activity in real time

2) Scalability Issues:

- Decentralization: Implement edge computing for real-time processing.
- Edge Computing: Process data locally to cut network load and latency.

3) Data Interoperability:

- Standards: Use open standards (e.g., MQTT, CoAP) for device communication.

C. Research Opportunities

Here we present several research directions that have not been fully explored:

- Enhanced Security & Privacy: Develop advanced encryption and protection for IoT.
- Energy Efficiency: Focus on low-power protocols and energy-harvesting for devices.
- AI & Edge Computing: Use AI and edge computing for real-time decisions without cloud dependency.
- Interoperability: Establish universal standards for device communication.
- 5G and Beyond: Leverage 5G to resolve bandwidth and latency issues in IoT.
- Edge Computing: Process data locally to reduce latency and improve efficiency.
- Blockchain: Ensure secure, decentralized data verification for sectors like healthcare.

While IoT faces challenges such as security and scalability, these issues also present opportunities for innovation. Solutions like blockchain for data security and 5G for scalability are already being developed and have the potential to revolutionize sectors like healthcare and smart cities.

- Personalized Medicine: Overcoming data interoperability and privacy challenges could enable seamless sharing of patient data between devices and healthcare providers, leading to more accurate diagnoses and personalized treatments.
- Industrial Automation: Addressing IoT scalability and real-time processing challenges could lead to fully automated manufacturing systems, reducing human intervention and increasing productivity.
- Environmental Monitoring: By resolving connectivity issues in remote areas, IoT could lead to significant advancements in environmental monitoring, such as more accurate predictions of natural disasters and optimized resource management.

VI. Conclusion

IoT presents significant opportunities in both healthcare and industrial applications, enabling enhanced productivity, better resource management, and improved decision-making. However, these opportunities come with considerable challenges, particularly in terms of security, reliability, and data management. By classifying IoT devices into mMTC and URLLC categories, we can better understand the specific needs of different applications and address these challenges accordingly. In healthcare, IoT offers the potential for better patient outcomes and more efficient care delivery, while in industrial settings, it promises greater automation and operational efficiency. To fully realize the potential of IoT in these sectors, it is crucial to continue addressing the technical, operational, and security challenges that remain.

References

[1] Laghari, Asif Ali, et al. "A review and state of art of Internet of Things (IoT)."Archives of Computational Methods in Engineering (2021):1-19.

[2] Zeinab, Kamal Aldein Mohammed, and Sayed Ali Ahmed Elmustafa. "Internet of things applications, challenges and related future technologies." World Scientific News 67.2 (2017): 126-148.

[3] Statista: Internet of Things (IoT) connected devices installed base worldwide from 2015 to 2025 (in billions) [Internet] (2024). https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Accessed 24 September 2024

[4] Khanh, Quy Vu, et al. "Wireless communication technologies for IoT in 5G: Vision, applications, and challenges." Wireless Communications and Mobile Computing 2022.1 (2022): 3229294.

[5] Bana, Alexandru-Sabin, et al. "Massive MIMO for internet of things (IoT) connectivity." Physical Communication 37 (2019): 100859.

[6] Saad, Joe. Evolution of mobile networks architecture and optimization of radio resource management. Diss. Université Paris-Saclay, 2024.

[7] Maluha, Dawid. Analysis of algorithms for encryption and integrity protection in 5G networks. Diss. Instytut Telekomunikacji, 2023.

[8] Kopetz, Hermann, and Wilfried Steiner. "Internet of things." Real-time systems: design principles for distributed embedded applications. Cham: Springer International Publishing, 2022. 325-341.

[9] Alves, Hirley, and Onel Alcaraz Lopez. "Wireless RF Energy Transfer in the Massive IoT Era: Towards Sustainable Zero-energy Networks." (2021).

[10] Raza, Usman, Parag Kulkarni, and Mahesh Sooriyabandara. "Low power wide area networks: An overview." ieee communications surveys & tutorials 19.2 (2017): 855-873.

[11] Mikhaylov, Konstantin, et al. "Energy efficiency of multi-radio massive machine-type communication (MR-MMTC): Applications, challenges, and solutions." IEEE Communications Magazine 57.6 (2019): 100-106.

[12] Ji, Hyoungju, et al. "Ultra-reliable and low-latency communications in 5G downlink: Physical layer aspects." IEEE Wireless Communications 25.3 (2018): 124-130.

[13] Ali, Rashid, et al. "URLLC for 5G and beyond: Requirements, enabling incumbent technologies and network intelligence." IEEE Access 9 (2021): 67064-67095.

[14] Hashemi, Ramin, et al. "Average rate and error probability analysis in short packet communications over RIS-aided URLLC systems." IEEE Transactions on Vehicular Technology70.10 (2021): 10320-10334.

[15] Khan, Benish Sharfeen, et al. "URLLC and eMBB in 5G industrial IoT: A survey." IEEE Open Journal of the Communications Society 3 (2022): 1134-1163.

[16] Farahani, Bahar, Farshad Firouzi, and Krishnendu Chakrabarty. "Healthcare iot." Intelligent Internet of Things: From Device to Fog and Cloud (2020): 515-545.

[17] Abadi, Marzieh Jalal, and Babak Hossein Khalaj. "Connectivity through Wireless Communications and Sensors." Industry 4.0 Vision for Energy and Materials: Enabling Technologies and Case Studies (2022): 3-58.

[18] Bhattacharya, Saurabh, and Manju Pandey. "Issues and Challenges in Incorporating the Internet of Things with the Healthcare Sector." Data Engineering and Communication Technology: Proceedings of ICDECT 2020 (2021): 639-651.

[19] Sahu, Gitimayee, and Sanjay S. Pawar. "Smart healthcare in smart city using wireless body area network and 5G." Networking Technologies in Smart Healthcare. CRC Press, 2022. 1-21..

[20] Kharche, Shubhangi, and Prajakta Dere. "Interoperability Issues and Challenges in 6G Networks." J. Mobile Multimedia18.5 (2022): 1445-1470..

[21] Peralta-Ochoa, Angélica M., et al. "Smart healthcare applications over 5G networks: A systematic review." Applied Sciences 13.3 (2023): 1469.

[22] Babaei, Aptin, Parham M. Kebria, and Saeid Nahavandi. "5G for Low-latency Human-Robot Collaborations; Challenges and Solutions." 2022 15th International Conference on Human System Interaction (HSI). IEEE, 2022.

[23] Yoshizawa, Takahito, Sheeba Backia Mary Baskaran, and Andreas Kunz. "Overview of 5G URLLC system and security aspects in 3GPP." 2019 IEEE Conference on Standards for Communications and Networking (CSCN). IEEE, 2019

[24] Jaidka, Himanshu, Nikhil Sharma, and Rajinder Singh. "Evolution of iot to iiot: Applications & challenges." Proceedings of the international conference on innovative computing & communications (ICICC). 2020..

[25] Wang, Bizhu, Yan Sun, and Xiaodong Xu. "A scalable and energy-efficient anomaly detection scheme in wireless SDN-based mMTC networks for IoT." IEEE Internet of Things Journal 8.3 (2020): 1388-1405.

[26] Elgarhy, Osama, et al. "Energy efficiency and latency optimization for IoT URLLC and mMTC use cases." IEEE Access (2024).

[27] Atharvan, Gannu, et al. "A way forward towards a technology - driven development of industry 4.0 using big data analytics in 5G - enabled IIoT." International journal of communication systems 35.1 (2022): e5014.

[28] Chen, Shuai, et al. "Exploring the global geography of cybercrime and its driving forces." Humanities and Social Sciences Communications 10.1 (2023): 1-10.

[29] Bashiir, Abdullahi Abdirahim. "Smart Cities and IOT for Sustainable Urban Development." *Research Output Journal of Biological and Applied Science* 3.1 (2024): 23-27.

[30] Sadeghi, Alireza, et al. "Digital Twins for Condition and Fleet Monitoring of Aircraft: Towards More-Intelligent Electrified Aviation Systems." *IEEE Access* (2024).